ABSTRACT OF THE DISCLOSURE

[0054] A method and system for ensuring security-compliant creation and signing of endorsement keys of manufactured TPMs. The endorsement keys are generated for the TPM. The TPM vendor selects an N-byte secret and stores the N-byte secret in the TPM along with the endorsement keys. The secret number cannot be read outside of the TPM. The secret number is also provided to the OEM's credential server. During the endorsement key (EK) credential process, the TPM generates an endorsement key, which comprises both the public key and a hash of the secret and the public key. The credential server matches the hash within the endorsement key with a second hash of the received public key (from the endorsement key) and the vendor provided secret. The EK certificate is generated and inserted into the TPM only when a match is confirmed.